UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/270,967	03/17/1999	DAVID GRABELSKY	98630	3345

20306 7590 03/29/2005

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 03/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/270,967	GRABELSKY ET AL.	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 January 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Response to Arguments

1. This communication is in response to applicants' amendment received on January 18, 2005.

2. Applicants are reminded that a declaration signed by all applicants has not been received yet.

3. Applicants' arguments have been fully considered but they are not persuasive.

4. On page 3 of remarks, applicants argue that: "Minear does not teach DNAT. In fact, Minear does not teach network translation in any form." And on page 4 of remarks, applicants argue that: "Minear simply does not disclose DNAT routers of claims 3, 11, 31, and 37."

On the contrary to the above arguments, Minear in Fig. 3 discloses a distributed network with workstations H1, H2 and H3 and firewalls SW1 and Sw2. Minear discloses that the IP addresses in both side of the firewalls are different. For example, the IP address of the workstation H1 within its private network is 172.17.0.0, but beyond the firewall SW1, in an unprotected network (i.e., Internet) is 192.168.20.1. This clearly indicates that the firewalls in the distributed network of Minear perform address translation and also perform as router. Therefore, Minear teaches DNAT and DNAT router.

6. On page 3 of remarks, last paragraph, applicants argue that: "contrary to independent claims 1, 9, 34, and 36 Minear fails to disclose requesting or receiving locally unique security values from a second network device on the same computer network to uniquely identify the first network device."

Minear teaches that a firewall (corresponding to the recited a second network device) selects a security association (SA) and a security parameters index (SPI) for the workstation (corresponding to the recited a first network device) on the same network that uniquely identify that workstation (col. 4, lines 29-58). Each SPI and SA which identify only one workstation correspond to the recited locally unique security values.

7. In light of the above submission, examiner maintains the previous claim rejections.

Previous claim rejections:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-39 are rejected under 35 U.S.C. 102(e) as being anticipated by Minear et al (5,983,350) (hereinafter Minear).

Referring to claims 1-4 and 9-12, Minear discloses a system and a method for regulating the flow of messages through a firewall (corresponding to the recited second network device) having a network protocol stack that includes an Internet protocol (IP) layer (abstract; col. 2, lines 50-60). Minear discloses that a security for communication between an end device (corresponding to the recited first network device) on one network and another end device (corresponding to the recited third network device) on a second network is provided by utilizing IPSEC (corresponding to the recited Internet Protocol security protocol) encryption and decryption work within the IP layer of the network protocol stack (col. 3, line 57-col. 4, line 7). Minear also discloses that the use of IPSEC requires a security association (col. 4, lines 8-28). Minear further discloses that users request the firewall administrator to setup SA's for their traffic (col. 6, lines 27-31). Thus, each device on the network receives its SA, which contains a security parameter index (SPI) (corresponding to the recited locally unique security value) from the firewall for secure communication with an end device on an external network (corresponding to the recited secure virtual connection).

Referring to claim 5, Minear discloses the use of an Encapsulated Security Payload (ESP) and an Authentication Header (AH) protocol for the secure traffic between a protected network and unprotected external network (col. 2, lines 1-5).

Referring to claims 6-8 and 13, Minear discloses a port is being assigned to each communicating device on the network based on a protocol (corresponding to the recited Port Allocation Protocol) (col. 2, lines 27-49; col. 3, lines 56-61, where the protocol stack includes a variety of protocols including a protocol port as indicated at col. 8, lines 5-10 and lines 42-53).

Referring to claims 14 and 15, Minear discloses:

A method for distributed network address translation using security, comprising the following steps:

Receiving a first message in a second secure protocol on a first network device on a first network to establish a secure virtual connection to the first network device from a third network device on a second external network (col. 4, lines 47-67);

Selecting a locally unique security value to use for the secure virtual connection from a list of locally unique security values, wherein the list of locally unique security values was received from a second network device on the first network with a first protocol (col. 4, lines 51-58; col. 9, lines 52-62); and

Sending a second message with second secure protocol to establish a secure virtual connection to the first network device on the first network from the third network device on the second external network wherein the second message includes the selected locally unique security value and security certificate sent to the first network device by the second network device (col. 2, line 65-col. 3, line 11; col. 3, line 66-col. 4, line 7; col. 4, lines 29-36).

Referring to claim 16, Minear discloses:

The method of Claim 14 wherein the list of one or more locally unique security values is a list of one or more security parameter indexes for Internet Protocol security protocol (col. 4, lines 8-12; col. 4, lines 59-64).

Referring to claim 17, Minear discloses:

The method of Claim 14 wherein the Internet Protocol security protocol is any of an Authentication Header protocol, Encapsulated Security Payload protocol, or an Internet Key Exchange Protocol (col. 2, lines 1-5).

Referring to claim 18, this claim is rejected as applied to the like elements of claim 6 as stated above.

Referring to claim 19, Minear discloses:

The method of Claim 14 wherein the secure virtual connection is an Internet Protocol security protocol security association (col. 4, lines 8-10' where IPSEC is an IP security protocol that uses an SA; col. 9, lines 30-32, where the tunnel between two hosts on two different network corresponds to the recited secure virtual connection.)

Referring to claims 20 and 21, Minear discloses:

Sending a request message in a second secure protocol from a first network device on a first network to a second network device on the first network, wherein the

request message in the second secure protocol includes security information (col. 6, lines 27-31; col. 4, lines 29-36, where the userid and address are security information);

Routing the request message from the second network device to a third network device on a second external network over a secure virtual connection between the first network device and the third network device (Fig. 3; col. 5, lines 20-25; col. 9, lines 30-32, where the tunnel between two hosts on two different network corresponds to the recited secure virtual connection);

Receiving a reply message in the second secure protocol from the third network device on the second network device on the first network for the first network device, wherein the reply message in the second secure protocol includes security information from the request message allocated by the second network device (col. 4, lines 7-67); and

Routing the reply message from the second network device to the first network device on the first network using one or more locally unique ports used for distributed network address translation (Fig. 3; col. 4, lines 47-58; col. 5, lines 344-46).

Referring to claim 22, Minear discloses:

The method of Claim 20 wherein the step of sending a request message in a second 5 secure protocol includes:

Constructing a virtual tunnel header for a local network address determined for the second network device (col. 52-62);

Prepending the virtual tunnel header to the request message, wherein the virtual tunnel header is used to create a virtual tunnel between the first network device and the second network device (col. 9, lines 28-32; col. 3, line 57-col. 4, line 8; col. 4, lines 17-18); and

Sending the request message to the second network device from the first network device over the virtual tunnel (col. 5, lines 47-64; Fig. 3).

Referring to claim 23 Minear discloses:

The method of Claim 20 wherein the step of routing the reply from the second network device to the first network device on the first network using the locally unique port from the reply in the second secure protocol includes:

Determining a local network address for the first network device using the locally unique port associated with the second network device (col. 4, lines 59-63, where the source IP address is the local network address);

Constructing a virtual tunnel header for the determined local network address for the first network device (col. 4, lines64-66);

Prepending the virtual tunnel header to the reply message, wherein the virtual tunnel header is used to create a virtual tunnel between the second network device and the first network device (col. 9, lines 28-32; col. 3, line 57-col. 4, line 8; col. 4, lines 17-18); and

Forwarding the reply message to the first network device from the second network device over the virtual tunnel (col. 6, lines 28-31).

Referring to claim 24, Minear discloses:

The method of Claim 23 wherein the local network address is an Internet Protocol address and the virtual tunnel header is an Internet Protocol tunnel header (col. 4, lines 8-19).

Referring to claim 25, Minear discloses the use of IPSEC protocol for the creation of secure association in response to the request a user (col. 4, lines 8-10; col. 4, lines 28-31).

Referring to claim 26, Minear discloses:

The method of Claim 25 wherein the Internet Protocol security protocol is any of an Authentication Header protocol, Encapsulated Security Payload protocol, or an Internet Key Exchange Protocol (col. 2, lines 1-5).

Referring to claim 27, Minear discloses:

The method of Claim 20 wherein the security information includes any of a locally unique security value or a security certificate (col. 4, lines 10-27.)

Referring to claims 28 and 29, Minear teaches:

Requesting one or more locally unique ports with a first message from a first protocol on a first network device from a second network device, wherein the one or more locally unique ports are used for distributed network address translation (col. 2,

lines 27-49; col. 3, lines 56-61, where the protocol stack includes a variety of protocols including a protocol port as indicated at col. 8, lines 5-10 and lines 42-53; col. 4, lines 8-28 and col. 6, lines 27-31, where a host machine request from a firewall to set up a unique SA for its traffic and the host machine and the firewall correspond to the recited first and second network devices);

Requesting one or more locally unique security values with a first message from the first protocol from the second network device, wherein the one or more locally unique security values are used with a second secure protocol to establish a secure virtual connection between the first network device and a third network device on a second external computer network and are used for distributed network address translation with security (col. 4, lines 8-36 and lines 59-66; col. 5, lines 13-18; col. 6, lines 27-31, where the IPSEC protocol establishes secure communication and the SPI is a unique secure value for the tunnel between two hosts);

Requesting a security certificate on the first network device from the second network device, wherein the security certificate includes a binding between a public encryption key and a combination of a network address for the first network device and the one or more locally unique ports and the second network device provides local security certificate services (col. 4, lines 8-36; col. 6, lines 27-31, where a host machine requests from a firewall to set up a SA that binds encryption keys and the network addresses and the SA corresponds to the recited security certificate);

Referring to claim 30, Minear teaches:

The method of Claim 28 wherein the one or more locally unique security values are security parameter indexes from an Internet Protocol security protocol (col. 4, lines 8-12, where IPSEC is the IP security protocol).

Referring to claim 31, Minear teaches:

The method of Claim 28 wherein the second network device is a distributed network address translation router (Fig. 1, where the firewall 14 is the second network device and corresponds to the recited router).

Referring to claim 32, Minear teaches:

The method of Claim 28 further comprising:

Establishing a secure virtual connection between the first network device and the third network device on the second external network using the security certificate (Fig. 3; col. 4, lines 8-28; col. 5, lines 13-18, where H1 and H2 are the first and the third network devices on two different networks and a SA that corresponds to the recited security certificate is used for virtual connection between the two host machines).

Referring to claim 33, Minear teaches:

The method of Claim 32, wherein the secure virtual connection is an Internet Protocol security protocol security association (col. 4, lines 8-28; col. 5, lines 13-18, where the secure connection is established by the IPSEC with a SA.)

Referring to claims 34 and 35, Minear teaches:

Sending one or more locally unique ports allocated on a second network device on a first computer network to a first network device on the first computer network with a second message from a first protocol wherein the one or more locally unique ports are used for distributed network address translator (col. 2, lines 27-49; col. 8, lines 5-10 and lines 42-53, where a ports are provided to the a host machine by a firewall to communicate to another machine on an external network);

Sending one or more locally unique security values allocated on the second network device to the first network device with a second message from the first protocol wherein the one or more locally unique security values are used with a second secure protocol to establish a secure virtual connection between the first network device and a third network device on a second external computer network and are used for distributed network address translation with security (col. 4, lines 8-28; col. 6, lines 27-31; col. 8, lines 5-10, where a security value is provided to a host machine by a firewall to have a secure virtual connection with another machine on an external network);

Sending a security certificate created on the second network device to the first network device, wherein the second network device provides local security certificate services on the first computer network and wherein the security certificate includes a binding for a public encryption key for the first network device and a combination of a network address for the first network device and the one or more locally unique ports allocated to the first network device to authenticate an identity for the first network device for a secure virtual connection between the first network device and a third

network device on a second external computer network (col. 4, lines 8-28; col. 6, lines 27-31, where the firewall provides SA that binds encryption keys with network addresses and corresponds to the recited security certificate to the host machine and it is used for authentication).

Referring to claims 36 and 37, Minear teaches:

A routing network device for allocating one or more locally unique ports, one or more locally unique security values and security certificates used for distributed network address translation with security for a plurality of other network devices, wherein the second network device provides local security certificate services and routing services for distributed network address translation with security (Fig. 3; col. 2, lines 27-49; col. 4, lines 8-28; col. 4, lines 59-66, where the firewall corresponds to the recited routing network device, the SPI corresponds to the recited security value and the SA corresponds to the recited security certificate); and

A network address table associated with the routing network device for mapping one or more locally unique security values to a network address for a network device (col. 4, lines 59-66; col. 7, lines 22-40); and

A security certificate for binding a public encryption key for the network device and a combination of a network address for the network device and one or more locally unique ports allocated to first network device by the routing network device to authenticate an identity for the network device for a secure virtual connection with external network device on an external computer network, wherein the security

certificate is issued by a second network device providing local security certificate services for distributed network address translation with security (col. 4, lines 8-28; col. 6, lines 27-31, where a firewall provides a host machine with a SA that binds encryption keys and the network addresses. The SA corresponds to the recited security certificate).

Referring to claim 38, Minear discloses:

The method of Claim 36 wherein the one or more locally unique security values are security parameter indexes from an Internet Protocol security protocol (col. 4, lines 8-28).

Referring to claim 39, Minear discloses:

The method of Claim 36 wherein the secure virtual connection is an Internet Protocol security protocol security association (col. 4, lines 8-28; col. 5, lines 13-18, where the secure connection is established by the IPSEC with a SA.)

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar
Examiner
Art Unit 2132

AN

March 24, 2005

GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100